Statement of Ronald L. Dick,
Director, National Infrastructure Protection Center
Federal Bureau of Investigation
before the
Senate Judiciary Committee
Subcommittee on Technology, Terrorism, and Government Information

July 25, 2001

Madame Chairperson, Ranking Member Kyl, and members of the subcommittee, thank you for inviting me here today to testify about the recommendations outlined in the General Accounting Office (GAO) report titled "CRITICAL INFRASTRUCTURE PROTECTION: Significant Challenges in Developing National Capabilities." Holding this hearing once again demonstrates your personal commitment to improving the security of our critical infrastructures and this subcommittee's leadership on this issue in Congress. Our work here is vitally important because the stakes involved are enormous. One recent study observed "12,085 attacks on over 5,000 distinct Internet hosts belonging to more than 2,000 distinct organizations during a three-week period."[1] My testimony today will address what has been accomplished and what still needs to be done to implement the GAO report's recommendations. Our assessment of the overall report is contained in our testimony of May 22, 2001 before this subcommittee.

At the outset, let me say how pleased I am here today with GSA's Assistant Commissioner Sallie McDonald of FedCIRC and Deputy Special Agent in Charge of the Financial Crimes Division Jim Savage of the U.S. Secret Service. Assistant Commissioner McDonald's statement explains in detail the close working relationship that GSA's FedCIRC has with the NIPC, so I won't dwell on that here.

The GAO's recommendations fell into several broad categories, including: enhancing capacity for strategic analysis; monitoring field implementation of NIPC performance measures; completing the Emergency Law Enforcement Services Sector Plan; improving cooperative relationships between the NIPC and its federal partners; and furthering information sharing between the NIPC, the Information Sharing and Analysis Centers (ISACs) and the public.

Nevertheless, the Center has made great strides in achieving its mission under Presidential Decision Directive (PDD)-63 over the past three years. In his prepared statement for the May 22, 2001 hearing, GAO's Director of Information Security, Mr. Robert F. Dacey, stated:

> First, the NIPC has provided valuable coordination and technical support to FBI field offices, which have established special squads and teams and one regional

---

[1]Danid Moore, Geoffrey M. Voelker and Stefan Savage, "Inferring Internet Denial-of-Service Activity," May 2001.

task force in its field offices to address the growing number of computer crime cases. The NIPC has supported these investigative efforts by (1) coordinating investigations among FBI field offices, thereby bringing a national perspective to individual cases, (2) providing technical support in the form of analyses, expert assistance for interviews, and tools for analyzing and mitigating computer-based attacks, and (3) providing administrative support to NIPC field agents. For example, the NIPC produced over 250 written technical reports during 1999 and 2000, developed analytical tools to assist in investigating and mitigating computer-based attacks, and managed the procurement and installation of hardware and software tools for the NIPC field squads and teams.

Over the past three years, NIPC has provided training for almost 4,000 participants. The NIPC's training program complements training offered by the FBI's Training Division as well as training offered by the Department of Defense and the National Cybercrime Training Partnership. Trained investigators are essential to our successfully combating computer intrusions.

Enhancing Capacity for Strategic Analysis

The GAO report recommended that the NIPC develop a comprehensive, written plan for strategic analysis. While we have numerous documents reflecting strategic and tactical planning, I agree that more work needs to be done. As the GAO report noted, our progress in this area has been impeded by the personnel shortfalls and management discontinuities within the interagency Analysis and Warning Section. I am pleased to report progress in this area with the arrival in April of a Central Intelligence Agency (CIA) senior officer, detailed for a sustained period as the Section Chief, and the recent selection of an National Security Agency (NSA) officer as the Chief of the Analysis and Information Sharing Unit within that section.

We have established four strategic directions for our capability growth through 2005: prediction, prevention, detection, and mitigation. None of these are new concepts but NIPC will renew its focus on each of them in order to strengthen our strategic analysis capabilities. NIPC will work to further strengthen its longstanding efforts on the early detection and mitigation of cyber attacks. These strategic directions will be significantly advanced by our intensified cooperation with federal agencies and the private sector. As the recent LEAVES and CODE RED worm incidents demonstrate, our working relations with key federal agencies, like FedCIRC, NSA, CIA, and the Joint Task Force - Computer Network Operations (JTF-CNO), and private sector groups such as SANS, the anti-virus community, and the major Internet service providers and backbone companies have never been closer. Our most ambitious strategic directions, prediction and prevention, are intended to forestall attacks before they occur. We are seeking ways to forecast or predict hostile capabilities in much the same way that the military forecasts weapons threats. The goal here is to forecast these threats with sufficient warning to prevent them. A key to success in these areas will be strengthened cooperation with intelligence collectors and the application of sophisticated new analytic tools to better learn from day-to-day

trends. The strategy of prevention is reminiscent of traditional community policing programs but with our infrastructure partners and key system vendors.

As we work on these four strategic directions: attack prediction, prevention, detection, and mitigation, we will have many opportunities to stretch our capabilities. With respect to all of these, the NIPC is committed to continuous improvement through a sustained process of documenting "lessons learned" from significant cyber events. We have already begun one such lessons learned study in connection with the recent LEAVES worm event. The NIPC also remains committed to achieving all of its objectives while upholding the fundamental rights of our citizenry, including the fundamental right to privacy.

The NIPC is excited by each of these strategic directions. I will lead a senior planning offsite later this summer and I expect to have the documented strategic plan completed by December. We are conducting this planning in a climate of intensified cyber attacks in by a growing number of automated tools that make effective hacking literally child's play. For instance, hackers are preying on the growing number of American home computer users for whom computers and cable modems are merely appliances rather than hobbies. These millions of home computers often lack the latest security updates, intrusion detection capabilities, and anti-virus signatures.

The GAO also recommended that the NIPC ensure that its Special Technologies and Applications Unit have the computer and communications resources necessary to analyze investigative data. The NIPC has already begun to address this issue by through the continued implementation of the NIPC's "data warehousing and data mining" project. This will allow the NIPC to retrieve incident data originating from multiple sources. Data warehousing includes the ability to conduct real-time all-source analysis and report generation. This initiative is ongoing and will require multiple year funding to reach maximum potential.

Monitoring Implementation of Field Performance Measures

The GAO recommended that the NIPC monitor implementation of new performance measures to ensure that they result in FBI Field Offices fully reporting information on computer crime complaints to the NIPC. The NIPC continues to monitor the open investigations of all the field offices and field performance in monthly statistical reports. Along with this, the FBI field offices report information on potential computer crimes by documenting and uploading reports of these incidents to the FBI's automated case support system. These records are searchable and available to NIPC Headquarters personnel who correlate the incidents with other pending investigations. The placement of the NIPC at the FBI endows the Center with both the authorities and the ability to combine law enforcement information flowing into the NIPC from the FBI Field Offices with other information streams derived from open, confidential, and classified sources. This capability is unique in the federal government. The NIPC views monitoring field office reporting as an ongoing action.

Completion of the Emergency Law Enforcement Services Plan

This task is completed. The NIPC serves as sector liaison for Emergency Law Enforcement Services (ELES) sector at the request of the FBI. The NIPC completed the ELES Sector Plan in February, 2001. The ELES Sector Plan was the first completed sector report under PDD-63 and was delivered to the White House on March 2, 2001. At the Partnership for Critical Infrastructure Security in Washington, D.C., in March, 2001, the ELES Plan was held up as a model for the other sectors. The NIPC also sponsored the formation of the Emergency Law Enforcement Services Sector forum, which meets quarterly to discuss issues relevant to sector security planning. The Forum contains federal, state, and local representatives. The next meeting of the forum is scheduled for September, 2001.

The Plan was the result of two years' work in which the NIPC surveyed law enforcement agencies concerning the vulnerabilities of their infrastructure. Following the receipt of the survey results, the NIPC and the ELES Forum produced the ELES Sector Plan. The NIPC also produced a companion "Guide for State and Local Law Enforcement Agencies" that provides guidance and a "toolkit" that law enforcement agencies can use when implementing the activities suggested in the Plan.

The importance of the ELES Sector Plan and the Guide cannot be overstated. These documents will aid some 18,000 police departments located in towns and neighborhoods to better protect themselves from attack. Since the local police are usually among the first responders to any incident threatening public safety, their protection is vital to our national security.

Enhancing Cooperative Relationships Among Federal Agencies

The GAO recommended that the NIPC formalize relationships between itself, other federal entities, and private sector ISACs, so a clear understanding of what is expected from the respective organizations exists. The NIPC has established effective information sharing and cooperative investigative relationships across the U.S. Government. A formal Memoranda of Agreement was just completed with the Department of Transportation's Federal Aviation Administration (FAA) which will govern how information is shared between FAA and NIPC and how that information will be communicated. This MOA formalizes a long-standing informal process of information sharing between NIPC and FAA. Informal arrangements have already been established with the Federal Communications Commission, Department of Transportation’s (DOT) National Response Center, DOT Office of Pipeline Safety, Department of Energy’s Office of Emergency Management, and others, which allow the NIPC to receive detailed sector-specific incident reports in a timely manner. Formal MOAs should soon be completed with several other agencies, including the National Coordinating Center for Telecommunications and the Federal Emergency Management Agency’s National Fire Administration.

The NIPC has developed into a truly interagency center and this in itself fosters cooperative relationships among agencies. It currently consists of detailees from the following U.S. government agencies: FBI, Army, Office of the Secretary of Defense (Navy Rear Admiral), Air Force Office of Special Investigations, Defense Criminal Investigative Service, National Security Agency, General Services Administration, United States Postal Service, Department of Transportation/Federal Aviation Administration, Central Intelligence Agency, Department of Commerce/Critical Infrastructure Assurance Office, and a representative from the Department of Energy. Canada, the United Kingdom, and Australia also each have a detailee in the Center.

The NIPC functions in a task force like way, coordinating investigations in a multitude of jurisdictions, both domestically and internationally. This is essential due to the transnational nature of cyber intrusions. As NIPC coordinates a myriad of investigative efforts within the FBI, it is not unlike the way the air traffic control system manages the stream of aircraft traffic across the United States and around the world.

To instill further cooperation and establish an essential deconfliction process among the investigative agencies, the NIPC asserted a leadership role by forming an Interagency Coordination Cell (IACC) at the Center. The IACC meets on a monthly basis and includes representation from U.S. Secret Service, NASA, U.S. Postal Service, Department of Defense Criminal Investigative Organizations (AFOSI, DCIS, NCIS, USACIDC), U.S. Customs, Departments of Energy, State and Education, Social Security Administration, Treasury Inspector General for Tax Administration and the CIA. The cell works to deconflict investigative and operational matters among agencies and assists agencies in combining resources on matters of common interest. The NIPC anticipates that this cell will expand to include all investigative agencies and inspectors general in the federal government having cyber critical infrastructure responsibilities. As we noted on May 22, 2001, the IACC has led to the formation of several task forces and prevented intrusions and compromises of U.S. Government systems.

Senior leadership positions in the NIPC are held by personnel from several agencies. The position of NIPC Director is reserved for a senior FBI executive. The Deputy Director of the NIPC is a two-star Navy Rear Admiral and the Executive Director is detailed from the Air Force Office of Special Investigations. The Section and Unit Chiefs in the Computer Investigation and Operations Section and the Training, Outreach, and Strategy Section are from the FBI. The Assistant Section Chief for Training, Outreach and Strategy is detailed from the Defense Criminal Investigative Service. The Section Chief of the Analysis and Warning Section is from the CIA and his deputy is a senior FBI agent. The head of the NIPC Watch and Warning Unit is reserved for a uniformed service officer, and the head of the Analysis and Information Sharing Unit is reserved for a National Security Agency manager.

While the Center has representatives from several U.S. Government agencies, staffing continues to be a challenge. Non-FBI personnel are provided to the Center on a non-reimbursable basis. Agencies have responded to the NIPC's requests for detailees by saying that they are constrained from sending personnel due to lack of funds. It is vitally important that

agencies be provided with sufficient funds for the assignment of detailees to the NIPC to support its strategic analysis mission.

As part of its emphasis on cooperation, the GAO recommended that the NIPC ensure that its Key Asset Initiative is integrated with the DoD and Critical Infrastructure Assurance Office (CIAO) programs. The objective of the Key Asset Initiative is to develop and maintain a database of information concerning "key assets" within each FBI Field Office's jurisdiction as part of a broader effort to protect the critical infrastructures against both physical and cyber threats. This initiative benefits national security planning efforts by providing a better understanding of the location, importance, and contact information for critical infrastructure assets across the United States. The NIPC has worked with the DoD and the CIAO on its Key Asset Initiative by involving them in the training of agents that work on the Initiative and by meeting with them regarding their programs. The NIPC and the Department of Defense are working toward a Memorandum of Understanding that will assist in defining cooperative efforts.

The NIPC has taken other initiatives as well in fulfilling its role to lead the critical infrastructure protection effort. This is evidenced by its coordinating actions as Chair of the Incident Response Sub-Group of the Information Infrastructure Protection and Assurance Group established by NSPD-1. The NIPC also routinely disseminates information through its participation in task forces and working groups that meet regularly. NIPC senior leadership participates in weekly senior level meetings to exchange strategic level information with the Assistant Secretary of Defense for Command, Control, Communication and Intelligence. Further collaboration is demonstrated through the NIPC's designation as chair of one of the subcommittees that is drafting version two of the National Plan.

The NIPC also maintains an active dialogue with the international community, to include its participation in the Trilateral Seminar of the International Cooperation for Information Assurance in Sweden and the G-8 Lyon Group (High Tech Crime Subgroup). NIPC has briefed visitors from a number of countries, including: Japan, Singapore, the United Kingdom, Germany, France, Norway, Canada, Denmark, Sweden, Israel, and other nations over the past year. In addition, NIPC personnel have accepted invitations to meet with government authorities in Sweden, Germany, Australia, the United Kingdom, and Denmark in recent months to discuss infrastructure protection issues with their counterparts. Finally, the NIPC Watch Center is connected to the Watch Centers of several of our close allies.

The NIPC sends out advisories on an ad hoc basis which are infrastructure warnings to address cyber or infrastructure events with possible significant impact. These are distributed to partners in private and public sectors. A number of recent advisories sent out by the NIPC (see for example Advisory 01-014, titled "New Scanning Activity {with W32-LEAVES.worm} Exploiting SubSeven Victims") serve to demonstrate the continued collaboration between the NIPC and its partner FedCIRC. The NIPC serves as a member of FedCIRC's Senior Advisory Council and has daily contact with that entity as well as a number of others including NSA and DoD's Joint Task Force - Computer Network Operations (JTF-CNO). On issues of national

concern, the recent incident involving the LEAVES and IDA CODE RED Worms are good examples of the NIPC's success in working with the National Security Council and our partner agencies to disseminate information and coordinate strategic efforts in a timely and effective manner.

In addition to its public web-based warning messages, the NIPC sends out tailored products to the federal government, the Information Sharing and Analysis Centers (ISACs), and InfraGard partners. Depending on the audience, these products may be classified or unclassified. The *Monthly Highlights* are sent out to policy/decision makers, and *Cybernotes* (which lists current exploited software vulnerabilities and other malicious code) is sent to system and network administrators. The *NIPC Daily Report* contains timely items of interest and significant cyber/infrastructure activity relevant to the infrastructure protection community and is sent to some of our federal partners as well as secure InfraGard members.

In response to PDD-63 provisions that all executive departments and agencies shall share with the NIPC information about threats and attacks on their systems, the NIPC-FAA MOU can serve as a forerunner for agreements to promote information sharing with the other 70 plus executive branch agencies. The NIPC has developed a model agreement can be modified to suit individual agency requirements. The execution of these agreements will confirm the obligations and clarify information sharing and warning procedures between the federal agencies and the NIPC. These model agreements will be communicated to federal executive branch agencies to open a dialogue on formalizing their relationship with the NIPC. These agreements will also address the GAO's recommendation that relationships between the NIPC and other federal entities be formalized so that a clear understanding of what is expected from the respective organizations exists. The NIPC anticipates that this will be an ongoing effort to create, monitor, and maintain these information sharing relationships.

Improving Information Sharing

The GAO report recommends that NIPC develop a plan to foster two-way exchange of information between the NIPC and the ISACs. The NIPC actively exchanges information with private sector companies, the ISACs, members of the InfraGard Initiative, and the public as part of the NIPC’s outreach and information sharing activities. Through NIPC's aggressive outreach efforts, we receive reports from many ISAC member companies. The NIPC has proven that it can properly safeguard their information and provide useful information in return. This reporting is partially responsible for the issuance of more warning products each year.

As noted in the GAO report, over the past two years the NIPC and the North American Electric Reliability Council (NERC)—the ISAC for the electric power sector—have established an indications, analysis and warning program (IAW) program, which makes possible the timely exchange of information valued by both the NIPC and the electric power sector. This relationship is possible because of a commitment both on the part of NERC and the NIPC to build cooperative relations. The close NERC-NIPC relationship is no accident but the result of

two interrelated sets of actions. First, as Eugene Gorzelnik, Director of Communications for the NERC, stated in his prepared statement at the May 22, 2001 hearing:

> [T]he NERC Board of Trustees in the late 1980s resolved that each electric utility should develop a close working relationship with its local Federal Bureau of Investigation (FBI) office, if it did not already have such a relationship. The Board also said the NERC staff should establish and maintain a working relationship with the FBI at the national level.

Second, the NIPC and NERC worked for over two years on building the successful partnership that now exists. It did not just happen. It took dedicated individuals in both organizations to make it happen. It is this success and dedication to achieving results that the NIPC is working to emulate with the other ISACs.

The NIPC also continues to meet regularly with ISACs from other sectors, particularly the financial services (FS-ISAC) and telecommunications (NCC-ISAC) ISACs, to establish more formal information sharing arrangements, drawing largely on the model developed with the electric power sector. In the past, information exchanges with these ISACs have consisted of a one-way flow of NIPC warning messages and products being provided to the ISACs. However, in recent months the NIPC has received greater participation from sector companies as they become increasingly aware that reporting to the NIPC enhances the value and timeliness of NIPC warning products disseminated to their sector. Productive discussions held this spring with the FS-ISAC, in particular, should significantly advance a two-way information exchange with the financial services industry. The NIPC is currently working with the FS-ISAC and the NCC-ISAC to develop and test secure communication mechanisms, which will facilitate the sharing of high-threshold, near real-time incident information. In the meanwhile we are working with these ISACs to share information. In March 2001, we were commended by the FS-ISAC for our advisory on e-commerce vulnerabilities (NIPC Advisory 01-003). According to the FS-ISAC, that advisory, coupled with the NIPC press conference on March 8, 2001, stopped over 1600 attempted exploitations by hackers the day immediately following the press conference.

ISACs have been established for the critical infrastructure sectors of banking and finance, information and telecommunications, electric power, and emergency law enforcement services. They have not yet been established for the remaining sectors enumerated in PDD-63. A model NIPC-ISAC agreement has been prepared to promote the sharing of information with these existing ISACs and ISACs yet to be formed. Agreements are being negotiated between the NIPC and the Telecommunications ISAC, as well as the NIPC and the United States Fire Administration (emergency fire services ISAC). The execution of these agreements should pave the way for NIPC agreements with other ISACs. The NIPC welcomes the participation of the sector lead agencies and the sector coordinators to improving the information sharing process with the ISACs. These efforts are ongoing.

The NIPC also shares information via its InfraGard Initiative. All 56 FBI field offices now have InfraGard chapters. Just in the last six months the InfraGard Initiative has added over 1000 new members to increase the overall membership to over 1600. It is the most extensive government-private sector partnership for infrastructure protection in the world, and is a service we provide to InfraGard members free of charge. InfraGard expands direct contacts with the private sector infrastructure owners and operators and shares information about cyber intrusions and vulnerabilities through the formation of local InfraGard chapters within the jurisdiction of each of the 56 FBI Field Offices and several of its Resident Agencies (subdivisions of the larger field offices).

A key element of the InfraGard initiative is the confidentiality of reporting by members. The reporting entities edit out the identifying information about themselves on the notices that are sent to other members of the InfraGard network. This process is called sanitization and it protects the information provided by the victim of a cyber attack. Much of the information provided by the private sector is proprietary and is treated as such. InfraGard provides its membership the capability to write an encrypted sanitized report for dissemination to other members. This measure helps to build a trusted relationship with the private sector and at the same time encourages other private sector companies to report cyber attack to law enforcement.

InfraGard held its first national congress from June 12-14, 2001. This conclave provided an excellent forum for NIPC senior managers and InfraGard members to exchange ideas. InfraGard's success is directly related to private industry's involvement in protecting its critical systems, since private industry owns almost all of the infrastructures. The dedicated work of the NIPC and the InfraGard members is paying off. InfraGard has already prevented cyber attacks by discretely alerting InfraGard members to compromises on their systems. On May 3, 2001, the InfraGard initiative received the 2001 WorldSafe Internet Safety Award from the Safe America Foundation for its efforts.

Conclusion:

I remain encouraged by the progress the NIPC has made in its first three years. Our multi-agency partnership has developed unique national capabilities that have never before been achieved. We will continually improve in the coming years in order to master the perpetually evolving challenges involved with infrastructure protection and information assurance. The GAO recommendations are all being addressed and I plan to keep the subcommittee updated on our progress. Thank you for inviting me here today and I welcome any questions you have.